BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Numéro de publication : **0 568 438 A1**

(12) DEMANDE DE BREVET EUROPEEN

(21) Numéro de dépôt : **93401084.4**

(51) Int. Cl.[5] : **G06F 12/14**

(22) Date de dépôt : **27.04.93**

(30) Priorité : **27.04.92 FR 9205187**

(43) Date de publication de la demande :
03.11.93 Bulletin 93/44

(84) Etats contractants désignés :
DE ES FR GB IT

(71) Demandeur : **GEMPLUS CARD INTERNATIONAL**
avenue du Pic de Bertagne, Parc d'activités de la Plaine de Jouques
F-13420 Gemenos (FR)

(72) Inventeur : **Stasi, Corinne, Cabinet BALLOT-SCHMIT**
7, rue Le Sueur
F-75116 Paris (FR)

(74) Mandataire : **Schmit, Christian Norbert Marie et al**
Cabinet Ballot-Schmit 7, rue Le Sueur
F-75116 Paris (FR)

(54) Procédé de sécurisation de programmes exécutables contre l'utilisation par une personne non habilitée et système sécurisé pour la mise en oeuvre du procédé.

(57) L'invention concerne un procédé de sécurisation de programme exécutable et notamment du programme de connexion à une station de travail. Le procédé consiste à cacher une clé dans une zone de données aléatoires verrouillant l'exécution du programme, le déchiffrement de l'adresse de cette clé ne pouvant être fait que par des personnes habilitées.

Application à la sécurisation de station de travail.

EP 0 568 438 A1

L'invention concerne un procédé de sécurisation de programmes exécutables contre l'utilisation par une personne non habilitée.

L'invention s'applique à tout programme exécutable par des moyens de traitement de données. Elle s'applique notamment à des programmes permettant d'établir une connexion avec un système informatique comme c'est le cas par exemple avec le système d'exploitation DOS et plus particulièrement avec le système d'exploitation UNIX utilisé généralement sur les stations de travail. On rappelle que l'on entend par station de travail, des postes individuels dédiés ayant une capacité de calcul importante permettant des applications telles que la CAO et fonctionnant généralement avec le système d'exploitation.

Il est en effet usuel que la connexion à une station de travail se fasse par un programme exécutable de connexion UNIX.

Le procédé conforme à l'invention s'applique avantageusement à la sécurisation de tels programme de connexion.

On rappelle également que dans le cas des stations de travail, le programme de connexion est exécuté pour initialiser une cession. Pour cela un utilisateur saisit à partir du clavier un nom d'utilisateur qui lui est propre et un mot de passe qui lui a été affecté. Les mots de passe et les noms d'utilisateurs des personnes habilitées à se connecter sont connus du système. S'il y a concordance entre les informations enregistrées préalablement et rentrées à partir du clavier alors le programme de connexion s'exécute et la connexion est établie.

Or il s'avère que de telles protections ne sont pas infaillibles car il arrive trop souvent que des personnes non habilitées parviennent à établir les connexions.

La présente invention permet de résoudre ce problème.

Elle a pour objet un procédé de sécurisation de tout programme exécutable par des moyens de traitement de données et notamment un procédé de sécurisation du programme de connexion à une station de travail.

La présente invention a plus particulièrement pour objet un procédé de sécurisation d'un programme exécutable par des moyens de traitement de données contre toute utilisation par une personne non habilitée.

Le procédé comporte à cette fin les étapes suivantes :

A) au préalable,

- choisir une clé dite clé mère permettant de verrouiller l'exécution du programme,
- calculer par chiffrement une adresse de mémorisation de la clé à l'intérieur d'un bloc de données aléatoires contenues dans le programme exécutable.
- mémoriser la clé à cette adresse,

B) lors des utilisations,

- déchiffrer l'adresse de la clé mère à partir de données d'identification et/ou d'authentification de la personne cherchant à lancer l'exécution du programme,
- identifier et/ou authentifier la personne lorsque le déchiffrement a eu lieu provoquant l'exécution du programme.

Selon une autre caractéristique du procédé la clé mère est une donnée aléatoire de n octets.

Selon une autre caractéristique, le calcul de l'adresse de mémorisation de la clé mère consiste à chiffrer cette clé avec une donnée unique au programme au moyen d'un algorithme de chiffrement, le résultat étant sur n octets.

Selon une autre caractéristique, la clé mère est éclatée en n adresses dans le bloc de données aléatoires

Selon une autre caractéristique, la clé est éclatée de manière à ce que chaque octet soit à l'adresse donnée par chaque octet des n octets d'adresse obtenus par chiffrement.

D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description détaillée qui est donnée à titre indicatif et nullement limitatif. Cette description se réfère à des dessins annexés sur lesquels :

- la figure 1, représente un schéma général de l'ensemble de sécurisation selon l'invention;
- la figure 2, représente un schéma d'organisation d'une mémoire de programme selon l'invention;
- la figure 3, représente un tableau illustrant les échanges entre carte à puce et moyens de traitement.

La figure 1 représente des moyens de traitement 1 représentés sous la forme d'un micro-ordinateur ou d'une station de travail reliés à une clavier 2. Bien entendu, ces moyens de traitement peuvent être toute autre système informatique capable d'exécuter un programme à sécuriser contre des utilisations non autorisées. Pour simplifier on parlera dans la suite de système.

La mémoire de programme a été symbolisée par une zone portant la référence 3 et est représentée de façon plus détaillée sur la figure 2.

Dans cette mémoire de programme 3 un ou plusieurs programmes ont été enregistrés. L'exécution de l'un au moins de ces programmes est verrouillée de manière à ne pouvoir être lancée que par des personnes habilitées. Pour cela le programme exécutable P, comporte une clé dite clé mère cachée dans une zone ZA de données aléatoires et déchiffrable seulement par une personne habilitée.

La clé mère est une donnée aléatoire entrée, dans le système par l'utilisateur habilité, au moment de l'installation du programme et, qui est cachée à une adresse dans cette zone ZA, obtenue par chiffre-

ment. L'adresse est chiffrée à partir de la clé mère et d'une donnée unique au programme.

Le chiffrement de l'adresse consiste par exemple à appliquer un algorithme DES (ou RSA) à la donnée formée par la clé mère et par la donnée unique au programme.

Selon un exemple préféré la donnée unique au programme est constituée par la date d'installation du programme dans le système, date donnée par le système et qui est bien unique à ce programme puisqu'elle tient compte de l'heure des minutes et des secondes et que la probabilité pour obtenir une même date est quasiment nulle.

De plus, selon un exemple préféré de réalisation la clé est éclatée de façon aléatoire dans la zone ZA.

La clé comporte n octets. Chaque octet se trouve réparti dans cette zone à une adresse qui est de ce fait également éclatée. L'adresse de chaque octet correspond à un octet du résultat du calcul de chiffrement. On peut se reporter au schéma de la figure 2 sur lequel on a représenté les emplacements AD de 8 octets dans la zone ZA, d'une clé mère ayant 8 octets à titre d'exemple.

La donnée unique, à savoir la date d'installation, est stockée à une adresse éclatée mais fixe dans la zone ZA connue du système de manière à ce que le système puisse retrouver la clé mère au moment voulu.

Lorsque dans un système un programme est ainsi sécurisé, les utilisateurs habilités ont, par le biais d'échanges d'informations secrètes, la possibilité de déverrouiller l'exécution de ce programme de la façon indiquée dans la suite.

Ainsi et de façon pratique chaque utilisateur possède une carte à mémoire dans laquelle sont enregistrés, un code secret connu uniquement par le titulaire de la carte, un nom d'utilisateur connu également par le titulaire de la carte, une clé de référence secrète.

Lorsqu'une personne habilitée désire lancer l'exécution du programme sécurisé, cette personne introduit sa carte 22 dans le lecteur 20 relié au système 1 puis, introduit à partir du clavier 2 du système son code secret et son nom d'utilisateur. Des échanges sont alors effectués entre le système et la carte par le biais du lecteur. Ces échanges sont représentés sur le tableau de la figure 3 et ont pour objet de réaliser le déchiffrement de la clé mère par toute personne habilitée qui est par conséquent authentifiée et autorisée. La clé mère (CL.M.) est cachée dans la zone ZA tel que décrit précédemment.

Le système calcule la clé de référence CL. REF à partir de CL.M. et du numéro de série lu sur la carte.

$$CL.\ REF = f(CL.M,\ n° Série)$$

La fonction f est de préférence pour tous les calculs de chiffrement réalisée par un algorithme de type DES ou RSA.

Après ce premier calcul, le système envoi une première donnée aléatoire : Alea 1, à la carte.

La carte calcule un résultat de chiffrement Rc à partir de Alea 1 et de CL. REF.

Le système calcule de son côté un résultat RS tel que :

$$Rs = f(CL.REF,\ Alea\ 1)$$

Le système reçoit de la carte une deuxième donnée aléatoire Alea 2 et le résultat Rc.

Le système compare Rs et Rc. Si ces résultats sont égaux alors la carte est authentifiée sinon elle est rejetée. On prend par la suite Rs = Rc = R.

Le système calcule alors une clé de session S.

$$S = f(R,\ Alea\ 2)$$

Le système envoi ensuite une donnée chiffrée Data, à la carte telle que :

$Data = f^{-1}(S,\ Code.Sec)$ où f^{-1} est l'inverse de f.

La carte calcule alors ensuite un résultat Rd tel que :

$$Rd = f(data,\ S)$$

La carte compare la donnée Rd et la donnée Code.Sec. enregistrées en mémoire pour savoir si le code rentré par l'utilisateur est identique à celui de la carte.

Lorsque c'est le cas l'utilisateur est authentifié. Il y a en fait une authentification réciproque entre le système et le titulaire de la carte.

La carte calcule alors un résultat Rn tel que :

$$Rn = f(NOM,\ S)$$

La donnée NOM est le nom d'utilisateur enregistré sur la carte.

Le résultat Rn est transmis au système qui déchiffre la donnée NOM en appliquant la fonction f^{-1} (inverse de f).

$$f^{-1}(Rn,\ S) = NOM$$

Si la donnée déchiffrée NOM est bien égale à la donnée NOM entrée par l'utilisateur alors, cet utilisateur est autorisé.

Lorsque l'authentification a eu lieu le programme s'exécute.

A l'installation du programme ainsi protégé, l'installateur dispose d'une carte installateur qui permet de mémoriser la clé mère que l'utilisateur habilité a entré dans le système à partir du clavier et qui est enregistrée dans la zone ZA, et de calculer la clé de référence à partir de cette clé mère et du numéro de série de la carte qui va être remise à l'utilisateur. La carte installateur est utilisée pour préparer les cartes utilisateurs. En effet, cette carte installateur est utilisée pour mémoriser les informations d'identification de la carte et de son titulaire à savoir : le code secret, le nom d'utilisateur, la clé de référence.

Comme cela a été dit précédemment le procédé s'applique notamment aux stations de travail. Il permet par exemple, dans ce cas, de sécuriser le mode d'accès à la station, le programme exécutable sécurisé étant alors le programme de connexion.

Le procédé pourra également être utilisé dans le cas de location de programme afin de réaliser un contrôle du nombre d'utilisation du programme par

simple comptage des accès à ce programme et verrouiller l'accès et donc l'exécution lorsque le nombre d'utilisation aura atteint une limite pré-enregistrée prévue par le contrat de location.

Revendications

1) Procédé de sécurisation d'un programme exécutable par des moyens de traitement de données contre toute utilisation par une personne non habilitée caractérisé en ce qu'il comprend les étapes suivantes :

A) au préalable,
- choisir une clé mère pour verrouiller l'exécution du programme,
- calculer par chiffrement une adresse de mémorisation de la clé à l'intérieur d'un bloc de données aléatoires contenues dans le programme exécutable,
- mémoriser cette clé mère à cette adresse,

B) lors des utilisations,
déchiffrer l'adresse de la clé mère à partir d'informations d'identification et/ou d'authentification de la personne cherchant à lancer l'exécution du programme,
- identifier et/ou authentifier la personne lorsque le déchiffrement a bien eu lieu pour provoquer l'exécution du programme.

2) Procédé de sécurisation selon la revendication 1, caractérisé en ce que la clé mère est une donnée aléatoire de n octets.

3) Procédé de sécurisation selon la revendication 2, caractérisé en ce que le calcul de l'adresse de mémorisation de la clé consiste à chiffrer cette clé avec une donnée unique au programme au moyen d'un algorithme de chiffrement, le résultat étant sur n octets.

4) Procédé de sécurisation selon l'une quelconque des revendications précédentes, caractérisé en ce que la clé mère est éclatée en plusieurs adresses dans le bloc de données aléatoires.

5) Procédé selon la revendication précédente, caractérisé en ce que la clé est éclatée de manière à ce que chaque octet soit à l'adresse donnée par chaque octet des n octets d'adresse obtenus par chiffrement.

6) Procédé selon l'une quelconque des revendications précédentes caractérisé en ce que la donnée unique de chaque programme est sa date d'installation dans les moyens de traitement.

7) Procédé selon l'une quelconque des revendications précédentes caractérisé en ce que l'étape d'identification et/ou d'authentification consiste à :
- fournir une carte à puce dans laquelle, on a au préalable mémorisé des informations d'identification et/ou d'authentification de la carte et du porteur.

8) Procédé selon la revendication 7 caractérisé en ce que les informations d'identification et d'authentification de la carte et du porteur comportent
- le n° de série de la carte,
- un nom d'identification du titulaire de la carte,
- un code secret connu du titulaire,
- une clé de référence fonction de la clé mère.

9) Procédé selon l'une quelconque des revendications précédentes caractérisé en ce que l'étape d'identification et/ou d'authentification consiste à réaliser une authentification réciproque entre la carte et le système et consiste pour la carte à :
- transmettre le n° de série de la carte aux moyens de traitement,
- calculer un premier résultat par chiffrement de la clé de référence résidente et d'un premier aléa reçu;
- à calculer un deuxième résultat (S) par chiffrement du résultat précédent et d'un deuxième aléa et à transmettre le premier résultat et le deuxième aléa;
- à calculer par chiffrement le code secret à partir d'une donnée (Data) reçue et du deuxième résultat,
- à comparer le code secret obtenu par le calcul et le code secret résident,
- à authentifier l'utilisateur dans le cas ou les deux codes sont identiques,
- à transmettre le nom du titulaire de la carte, chiffré,

et pour les moyens de traitement à :
- calculer la clé de référence par chiffrement du numéro de série à partir de la clé mère,
- à transmettre un premier aléa,
- à calculer un résultat par chiffrement du premier aléa et de la clé de référence obtenue,
- à comparer ce résultat avec le premier résultat obtenu dans la carte,
- à calculer une clé de session par chiffrement du résultat et du deuxième aléa,
- à calculer une donnée (Data) par déchiffrement de la clé de session et du code secret rentré par l'utilisateur,
- à transmettre cette donnée (Data) à la carte,
- à déchiffrer le nom reçu de la carte et comparer avec le nom rentré

10) Système informatique sécurisé caractérisé en ce qu'il comporte des moyens de traitement comprenant une mémoire de programme dans laquelle sont enregistrés un ou plusieurs programmes exécutables, les moyens étant reliés à un clavier et à un lecteur de carte caractérisé en ce que la mémoire de programme comporte une zone dans laquelle au moins un programme exécutable est sécurisé, son exécution ne pouvant avoir lieu que sous condition d'habilitation; en ce que pour cela le programme comporte une clé mère enregistrée à une adresse chiffrée à l'intérieur d'un bloc de données aléatoires de la zone dans laquelle est enregistré le programme,

et en ce que les cartes des utilisateurs habilités comportent une clé de référence fonction de la clé mère permettant aux moyens de traitement de déchiffrer l'adresse de la clé mère et d'identifier et/ou d'authentifier le titulaire de la carte déverrouillant ainsi l'exécution du programme.

11) Système informatique selon la revendication 10, caractérisé en ce que les moyens de traitement comprennent une station de travail et en ce que le programme sécurisé est le programme de connexion à la station de travail.

FIG_1

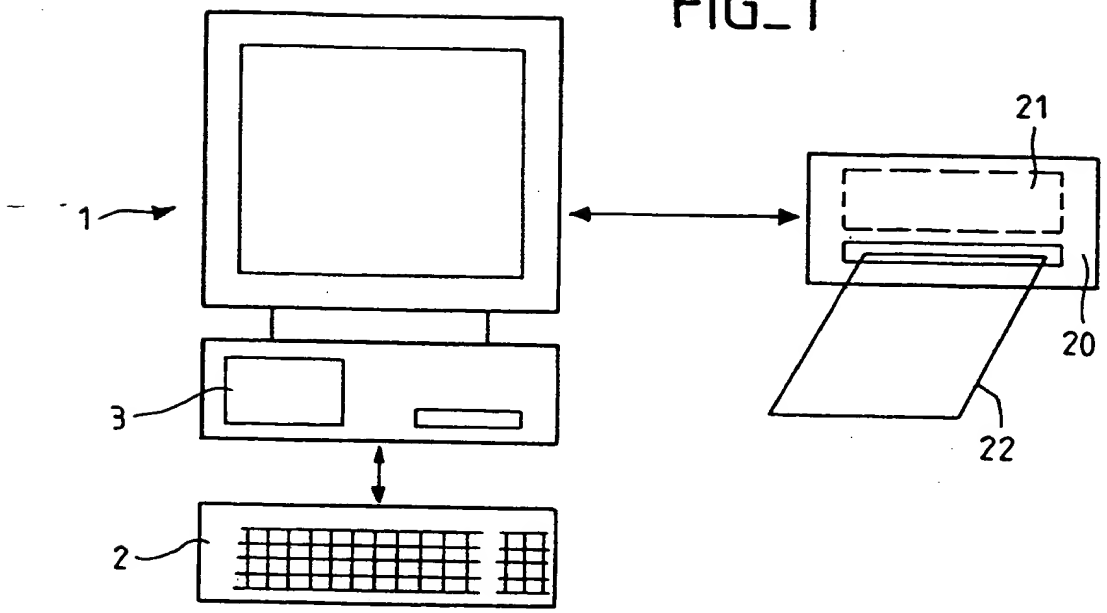

1
21
20
3
22
2

FIG_2

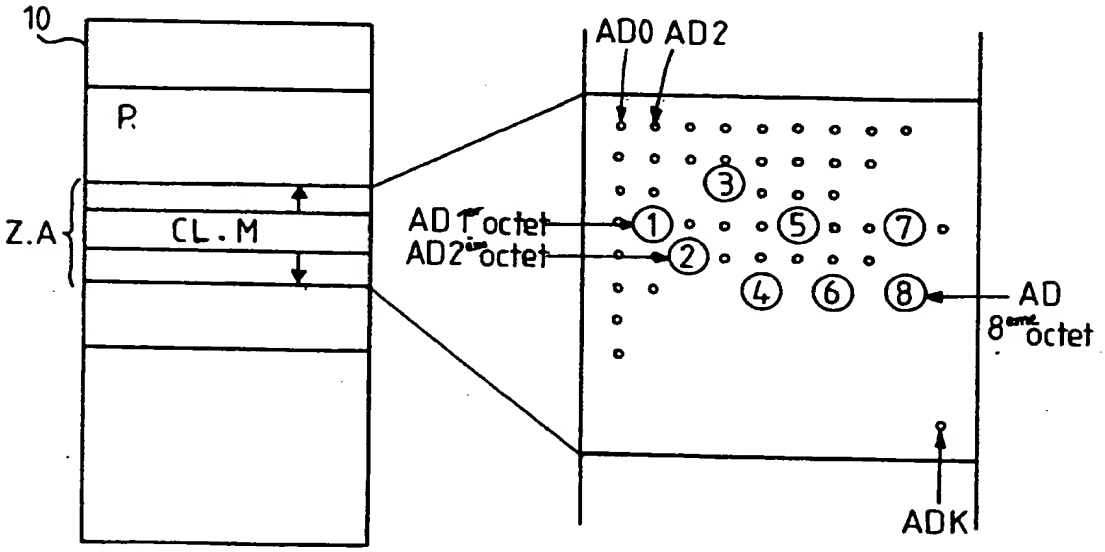
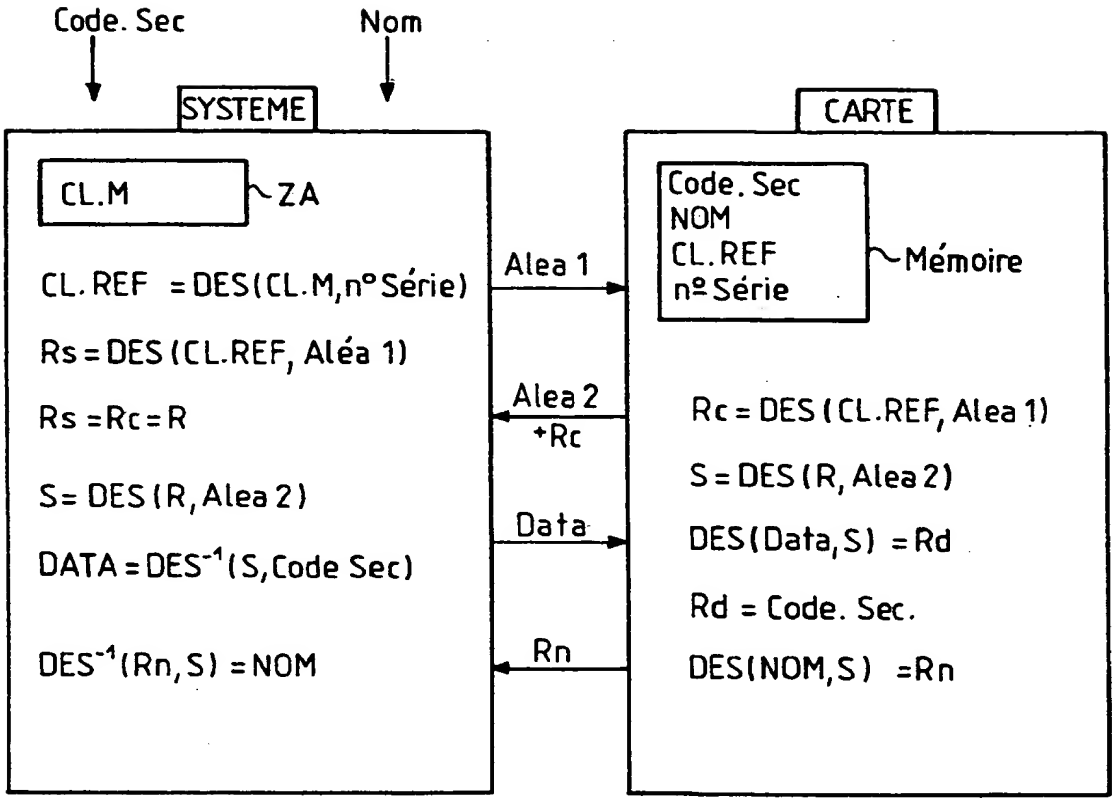

10
P.
Z.A
CL.M
AD0 AD2
AD 1er octet
AD 2ème octet
AD 8ème octet
ADK

FIG_3


Code. Sec
Nom
SYSTEME
CARTE
CL.M
ZA
CL. REF = DES(CL.M, n° Série)
Rs = DES (CL.REF, Aléa 1)
Rs = Rc = R
S = DES (R, Alea 2)
DATA = DES⁻¹ (S, Code Sec)
DES⁻¹ (Rn, S) = NOM
Alea 1
Alea 2
+Rc
Data
Rn
Code. Sec
NOM
CL. REF
n° Série
Mémoire
Rc = DES (CL.REF, Alea 1)
S = DES (R, Alea 2)
DES (Data, S) = Rd
Rd = Code. Sec.
DES (NOM, S) = Rn

Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numero de la demande

EP 93 40 1084

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (Int. Cl.5)
A	GB-A-2 205 667 (NCR) * abrégé * * page 8, ligne 15 - page 13, ligne 21 * * figures 3,5-9 *	1,2,7,10	G06F12/14
A	EP-A-0 339 115 (SIEMENS) * le document en entier *	1,7,10	
A	US-A-4 944 008 (PIOSENKA ET AL.) * le document en entier *	1,2,10	
			DOMAINES TECHNIQUES RECHERCHES (Int. Cl.5)
			G06F

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
BERLIN	04 AOUT 1993	MASCHE C.

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P0402)